On witnessing arbitrary bipartite entanglement in a measurement device independent way

Arindam Mallick[1, *] and Sibasish Ghosh[1, †]

[1]*Optics and Quantum Information Group, The Institute of Mathematical Sciences,*
HBNI, C. I. T. Campus, Taramani, Chennai 600113, India

Experimental detection of entanglement of an arbitrary state of a given bipartite system is crucial for exploring many areas of quantum information. But such a detection should be made in a device independent way if the preparation process of the state is considered to be faithful, in order to avoid detection of a separable state as entangled one. The recently developed scheme of detecting bipartite entanglement in a measurement device independent way [Phys. Rev. Lett **110**, 060405 (2013)] does require information about the state. Here by using Auguisiak et al.'s universal entanglement witness scheme for two-qubit states [Phys. Rev. A **77**, 030301 (2008)], we provide a universal detection scheme for two-qubit states in a measurement device independent way. We provide a set of universal witness operators for detecting NPT-ness(negative under partial transpose) of states in a measurement device independent way. We conjecture that no such universal entanglement witness exists for PPT(positive under partial transpose) entangled states. We also analyze the robustness of some of the experimental schemes of detecting entanglement in a measurement device independent way under the influence of noise in the inputs (from the referee) as well as in the measurement operator as envisazed in ref. [Phys. Rev. Lett **110**, 060405 (2013)].

I. INTRODUCTION:

Entanglement is shown to be a resource for quantum information proccesing, like quantum cryptography [1], telepotation [2], quantum metrology [3], channel capacity [4, 5]. Moreover, it helps to speed up computation sometimes [6] over the existing classical algorithms. Also, understanding entanglement is neccessary to reveal various non-classical nature of the physical world. Entanglement in quantum theory correlates two parties in such a way that at the individual levels, they lose their independent state descriptions. Mathematically, two parties $\mathcal{A}$ and $\mathcal{B}$ are separable iff their joint state ρ can be expressed as $\sum_j \alpha_j \ \rho_{\mathcal{A}}{}^j \otimes \rho_{\mathcal{B}}{}^j$ acting on the Hilbert space $\mathcal{H}_{\mathcal{AB}} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $\sum_j \alpha_j = 1$ and $0 \leq \alpha_j \leq 1$ $\forall j$, $\rho_{\mathcal{A}}{}^j$ and $\rho_{\mathcal{B}}{}^j$ are density matrices acting on $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{H}_{\mathcal{B}}$ respectively. If the joint state can't be written in the above form, we call them entangled [7].

Deciding whether a unknown state of a given bipartite quantum system is entangled or separable, remains as a challenging problem [8–10] right from the initial stage of quantum information theory. People tried to see the presence of entanglement in a state experimentally through some Bell-inequality violation, but there are entangled states which do not violate any such inequality [11]. Given any entangled state $\rho_{\mathcal{AB}}$, it is (in principle) possible to find out an entanglement witness observable W_ρ, whose measurement can distinguish the given entangled states from all possible separable states of the system, and the measurement is, in principle, implementable experimentally, even using local measurement settings, (possibly) supported by classical communication. It may be noted that an entanglement witness is a hermitian operator $W : \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \rightarrow \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ such that there exists atleast one entangled state $\rho_{\mathcal{AB}}$ on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, for which $\mathrm{Tr}[W\rho_{\mathcal{AB}}] < 0$ while $\mathrm{Tr}[W\sigma_{\mathcal{AB}}] \geqslant 0$ for all separable density matrices $\sigma_{\mathcal{AB}}$ on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. So W witnesses the entanglement in the state $\rho_{\mathcal{AB}}$. But $\mathrm{Tr}[W\sigma_{\mathcal{AB}}] \geqslant 0$ does not necessarily imply $\sigma_{\mathcal{AB}}$ is separable [12]. In general, W_ρ depends on the the form of entangled state $\rho_{\mathcal{AB}}$, and hence it does not have a universal character. Thus a state-independent witness operator is a desired one for most practical purposes.

The conventional entanglement detection strategies are based on the local measurement on each subsystem $\mathcal{A}$ and $\mathcal{B}$. In this case, perfectness of both the local measuring apparatuses is necessary. In fact, if some measurement results get lost or some over counting occurs in the measurement, it may lead to an erroneous conclusion about the entanglement of the state $\rho_{\mathcal{AB}}$. In ref. [13], time shift attack has been used experimentally which causes identification of a separable state as an entangled one. Such a scenario can be avoided if one can witness entanglement in a measurement device independent way.

Recently, Branciard et al. [14] demonstrated implementation of any entanglement witness operator in a measurement-device-independent way using Buscemi's work on semi-quantum nonlocal game [15]. This scheme of Branciard et al. [14] guaranteed that no separable state will be detected as an entangled state, irrespective of the kind of noise effects present during the measurement [14]. But their scheme depends on the form of the shared entangled state. Hence their witness operator lacks universal character, that is, it is unable to detect entanglement in a unknown state of the bipartite system.

Augusiak et al. [16] showed the existence of a universal entanglement witness operator that can detect entanglement in any two-qubit state, depending on the Peres-

arXiv:1506.03985v2 [quant-ph] 11 Jan 2017

Horodecki PPT criteria [7, 17]. But this does not address measurement device independent implementation of the witness operator, and moreover it is restricted to two-qubit case only.

In this paper, we claim that this two-qubit universal entanglement witness operator of Augusiak et al. [16] can be implemented in a measurement device independent way. We then generalize this idea for higher dimensional bipartite NPT entangled states and find out a set of finite number of universal NPT witnesses for any *given* bipartite system. We conjecture that no universal entanglement witness operator can exist to detect entanglement in a PPT entangled state. We also point out that, in the aforesaid scheme of Branciard et al.'s measurement device independent entanglement witness scheme [14], if some general type of noise is added with the inputs or with the measurement operator, the referee will not face any problem in witnessing entanglement provided he knows the character of the noise (here we will provide analysis for a particular type of noise and general treatment in appendix VII A). In case the referee doesn't know, we show how robust the witnessing operation can be dealt with.

Our article is organized as follows. In section II, we describe measurement device independent (MDI) scheme of entanglement witness (EW). Section III is devoted to MDI implementation of the two-qubit universal EW of Auguisiak et al. [16]. IV describes universal witness for NPT-ness of two-qudit states. Section V, describes the conjecture about the impossibility of the existence of universal witness operator for bipartite PPT-entangled states. In section VII A, we analyse the possible noise effects in measurement and inputs. We draw the conclusion of our work in section VII.

II. MEASUREMENT DEVICE INDEPENDENT(MDI) SCHEME OF ENTANGLEMENT WITNESS (EW) :

This scheme starts as a cooperative game played between two parties Alice($\mathcal{A}$) and Bob($\mathcal{B}$), who receive quantum states $\{\tau_s \in \mathcal{H}_{\mathcal{A}_\mathcal{O}}\}$ and $\{\omega_t \in \mathcal{H}_{\mathcal{B}_\mathcal{O}}\}$ respectively as inputs from a referee, who then ask them to produce outputs a and b respectively. Here $\dim(\mathcal{H}_{\mathcal{A}_\mathcal{O}})$ = $\dim(\mathcal{H}_\mathcal{A})$= $d_\mathcal{A}$ and $\dim(\mathcal{H}_{\mathcal{B}_\mathcal{O}}) = \dim(\mathcal{H}_\mathcal{B}) = d_\mathcal{B}$ and for our analysis, we consider $d_\mathcal{A} = d_\mathcal{B} = d$. During the game, Alice and Bob aren't allowed to communicate anyway, but before starting the game they have to decide their strategies where they may share apriori a bipartite state $\rho_{\mathcal{AB}}$. If the state $\rho_{\mathcal{AB}}$ is entangled state they can always get an average pay-off which is more than the case when $\rho_{\mathcal{AB}}$ is any separable state. So, from the average pay-off values, the referee can conclude whether the corresponding shared state was entangled or separable (by knowing the maximum average payoff for all possible separable states). To produce outcomes of the game, each party has to perform local joint projective measurement
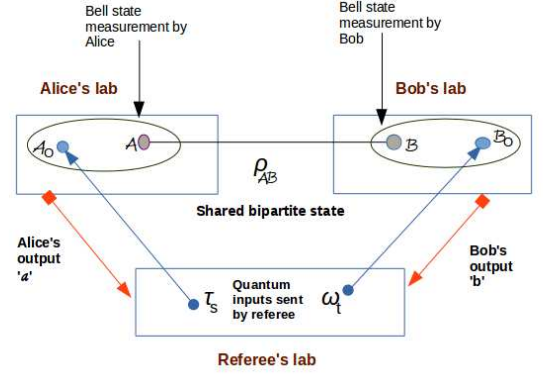

FIG. 1: (colour online) Alice and Bob performs Bell state measurement on the states of the joint systems $\mathcal{A}_\mathcal{O}\mathcal{A}$ and $\mathcal{B}\mathcal{B}_\mathcal{O}$ respectively. Blue arrows are lossless quantum channels for sending input states to Alice and Bob. Red arrows correspond to the lossless classical channels for receiving the outputs. Green ellipces indicate joint Bell state measurement performed by the players.

on their individual inputs and their individual subsystems of the shared state, see Figure 1 for details.

The authors of [14] described the aforesaid projective measurement in the maximally entangled state

$$|\Phi\rangle_{\mathcal{A}_\mathcal{O}\mathcal{A}} = |\Phi\rangle_{\mathcal{B}\mathcal{B}_\mathcal{O}} = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jj\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d,$$

with probability of output $(a,b) = (1,1)$ for given quantum input pair (τ_s, ω_t) being $P_{\rho_{\mathcal{AB}}}(1,1|s,t) = \mathrm{Tr}\Big((|\Phi\rangle_{\mathcal{A}_\mathcal{O}\mathcal{A}}\langle\Phi| \otimes |\Phi\rangle_{\mathcal{B}\mathcal{B}_\mathcal{O}}\langle\Phi|)(\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t)\Big)$, and showed that if the average payoff function, $\Pi(\rho_{\mathcal{AB}}) = \sum_{s,t}\tilde{\beta}_{s,t}P_{\rho_{\mathcal{AB}}}(1,1|s,t)$ then

$$I(\rho_{\mathcal{AB}}) := \max\big\{\Pi(\sigma_{\mathcal{AB}})\big\} - \Pi(\rho_{\mathcal{AB}})$$

$$= \max_{\sigma_{\mathcal{AB}}}\Big\{\sum_{s,t}\tilde{\beta}_{s,t}P_{\sigma_{\mathcal{AB}}}(1,1|s,t)\Big\} - \sum_{s,t}\tilde{\beta}_{s,t}P_{\rho_{\mathcal{AB}}}(1,1|s,t)$$

$$= \sum_{s,t}\beta_{s,t}P_{\rho_{\mathcal{AB}}}(1,1|s,t). \tag{1}$$

where, the maximization is performed over all possible separable state $\sigma_{\mathcal{AB}}$ of the bipartite system. The outcome $(1,1)$ is nothing but the successful projection on the state $\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t$ by the tensor product of the operator $|\Phi\rangle_{\mathcal{A}_\mathcal{O}\mathcal{A}}\langle\Phi| \otimes |\Phi\rangle_{\mathcal{B}\mathcal{B}_\mathcal{O}}\langle\Phi|$ and $\beta_{s,t}$ is pay-off value corresponding to the input state (τ_s, ω_t).

If we want to use $I(\rho_{\mathcal{AB}})$ as a signature of entanglement witness, it has to be proportional to $\mathrm{Tr}[W\rho_{\mathcal{AB}}]$, and the witness operator W needs to be expressed as a linear combination of the tensor product of the transposed input states,

$$W = \sum_{s,t}\beta_{s,t}\tau_s^T \otimes \omega_t^T, \tag{2}$$

which, in principle, is possible in this case as the inputs τ_s (to Alice) and ω_t (to Bob)-supplied by the referee- are sufficient enough to span the respective vector space of witness operators on $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Then the referee will determine the values of $\beta_{s,t}$ accordingly prior to the game, such that he can identify whether the shared state is entangled from the sign of $I(\rho_{\mathcal{AB}})$. Indeed this can be done as W is hermitian and transposed input density matrices are also hermitian. The referee just have to choose the input states τ_s and ω_t in order to form a complete set of operators $\{\, \tau_s^T \otimes \omega_t^T \,\}$ to express W as a linear combination of these operators.

In this scenario, accuracy in preparation of the input states must be trusted. In ref. [14], it is proved that no noise introduced in the local measurement operator can lower the bound $I(\rho_{\mathcal{AB}}) \geq 0$ for separable $\rho_{\mathcal{AB}}$, so, in this scheme, separable state will never be identified as an entangled one. In this sense the scheme of ref. [14] is measurement device independent.

A. Detecting entanglement in unknown two-qubit state :

In the case of witnessing in a unknown two-qubit state [16], instead of sharing single copy of the state, the players need to share four identical copies of the state. This is so because the signature of $\det(\rho_{\mathcal{AB}}^{T_\mathcal{B}})$ = product of eigenvalues of $\rho_{\mathcal{AB}}^{T_\mathcal{B}} = \mathrm{Tr}[W\rho_{\mathcal{AB}}^{\otimes 4}] = \lambda_1\lambda_2\lambda_3\lambda_4$, completely determines whether the two-qubit state $\rho_{\mathcal{AB}}$ is entangled or separable. Here λ_i's are eigenvalues of $\rho_{\mathcal{AB}}^{T_\mathcal{B}}$ and W is a hermitian operator acting on $\mathcal{H}_\mathcal{A}^{\otimes 4} \otimes \mathcal{H}_\mathcal{B}^{\otimes 4}$ (with $\dim \mathcal{H}_\mathcal{A}$ = $\dim \mathcal{H}_\mathcal{B}$ = 2). From the Newton-Girard formula [18], we have : $\lambda_1\lambda_2\lambda_3\lambda_4 =$

$$\frac{1}{24}\left(1 - 6\sum_{i=1}^{4}\lambda_i^4 + 8\sum_{i=1}^{4}\lambda_i^3 + 3\left(\sum_{i=1}^{4}\lambda_i^2\right)^2 - 6\sum_{i=1}^{4}\lambda_i^2\right)$$

To formulate this in terms of an operator, we first use the swap operator $V^{(k)}$, defined as

$$V^{(k)}\big(|\phi_1\rangle_{\mathcal{A}_1\mathcal{B}_1} \otimes |\phi_2\rangle_{\mathcal{A}_2\mathcal{B}_2} \otimes \,....\, |\phi_k\rangle_{\mathcal{A}_k\mathcal{B}_k}\big)$$
$$= |\phi_k\rangle_{\mathcal{A}_1\mathcal{B}_1} \otimes |\phi_1\rangle_{\mathcal{A}_2\mathcal{B}_2} \otimes \,....\, |\phi_{k-1}\rangle_{\mathcal{A}_k\mathcal{B}_k} \qquad (3)$$

with the property $\mathrm{Tr}(V^{(k)}\rho^{\otimes k}) = \mathrm{Tr}(\rho^k)$ [16, 19, 20] for any hermitian matrix ρ and $V^{(k)}$ is not, in general, a hermitian operator except for $k = 2$. So to make it an observable in place of $V^{(k)}$, $\frac{1}{2}(V^{(k)} + V^{(k)\dagger})$ will be used for farther analysis. As the swap operator $V^{(k)}$ is a real matrix with respect to a fixed basis, used for the whole analysis,

$$\mathrm{Tr}((\rho_{\mathcal{AB}}^{T_\mathcal{B}})^k) = \mathrm{Tr}(V^{(k)}(\rho_{\mathcal{AB}}^{T_\mathcal{B}})^{\otimes k})$$
$$= \frac{1}{2}\mathrm{Tr}\Big((V^{(k)} + V^{(k)\dagger})^{T_\mathcal{B}}\rho_{\mathcal{AB}}^{\otimes k}\Big)$$
$$= \frac{1}{2}\mathrm{Tr}\Big(\big[\,\tilde{V}^{(k)} \otimes \tilde{V}^{(k)T} + \tilde{V}^{(k)T} \otimes \tilde{V}^{(k)}\,\big]\rho_{\mathcal{AB}}^{\otimes k}\Big),$$
$$\text{where } \tilde{V}^{(k)} : \mathcal{H}_j^{\otimes k} \to \mathcal{H}_j^{\otimes k}$$

is given by :

$$\tilde{V}^{(k)}\big(|\phi_1\rangle_{j_1} \otimes |\phi_2\rangle_{j_2} \otimes \,......\, \otimes |\phi_k\rangle_{j_k}\big)$$
$$= |\phi_k\rangle_{j_1} \otimes |\phi_1\rangle_{j_2} \otimes \,......\, \otimes |\phi_{(k-1)}\rangle_{j_k} \quad \text{for } j = \mathcal{A}, \mathcal{B}. \quad (4)$$

Then, hermitian operator witnessing entanglement in arbitrary two-qubit state, is given by,

$$W^{\mathrm{univ}} = \frac{1}{24}\mathbb{I}_{256 \times 256} - \frac{1}{8}\left(\tilde{V}^{(4)} \otimes \tilde{V}^{(4)T} + \tilde{V}^{(4)T} \otimes \tilde{V}^{(4)}\right) + \frac{1}{6}\mathbb{I}_{4\times 4} \otimes \left(\tilde{V}^{(3)} \otimes \tilde{V}^{(3)T} + \tilde{V}^{(3)T} \otimes \tilde{V}^{(3)}\right)$$
$$+ \frac{1}{8}V^{(2)} \otimes V^{(2)} - \frac{1}{4}\mathbb{I}_{16\times 16} \otimes V^{(2)}, \qquad (5)$$

and our $I(\rho_{\mathcal{AB}})$ turns out to be proportional to $\mathrm{Tr}(W^{\mathrm{univ}}\rho_{\mathcal{AB}}^{\otimes 4}) = \det(\rho_{\mathcal{AB}}^{T_\mathcal{B}})$, see the next section III.

The above form of witness operator doesn't depend on the type of two-qubit shared state, so that entanglement in an unknown state can be detected. In this sense it's universal entanglement witness operator.

III. MDI IMPLEMENTATION OF TWO-QUBIT UNIVERSAL EW :

Recent work by Bartkiewicz et al. in [21] demonstrated the implementation of the aforesaid universal entanglement witness operator (5) for two-qubit case, using photon polarized states. But that has not been done in a measurement device independent way.

Authors of ref. [22] and [23], address entanglement de-

tection of arbitrary two-qubit states in MDI way, but their approach focus on optimization of entanglement witness operator instead of the question of the universality of that, as we discuss throughout this article.

The game of Fig 1, starts with two inputs (one for Alice and one for Bob) and single copy of a shared state, while our universal measurement scheme for witnessing entanglement needs four identical copies of shared state $\rho_{\mathcal{AB}}$ at each run of the experiment and the witness operator W^{univ} is a 256×256 dimensional matrix. Thus, the input Hilbert space is $[\mathbb{C}^2]^{\otimes 4} \otimes [\mathbb{C}^2]^{\otimes 4} = \mathbb{C}^{16} \otimes \mathbb{C}^{16}$ instead of $\mathbb{C}^2 \otimes \mathbb{C}^2$. As a result of that, both τ_s and ω_t must be density matrices on $\mathbb{C}^{16}$.

So, the witness operator W^{univ} of equ. (5) should be of the form,

$$W^{\mathrm{univ}} = \sum_{s,t} \beta_{s,t} (\tau_s^T \otimes \omega_t^T), \qquad (6)$$

where, the input states τ_s and ω_t are expandable in appropriate Gell-mann matrix basis such that

$$\tau_s^T = \frac{\vec{\Lambda}.\mathrm{Tr}(\tau_s^T \vec{\Lambda})}{16} = \sum_i \Lambda_i \; p_i^{(s)},$$

$$\omega_t^T = \frac{\vec{\Lambda}.\mathrm{Tr}(\omega_t^T \vec{\Lambda})}{16} = \sum_j \Lambda_j \; q_j^{(t)}, \qquad (7)$$

where $\vec{\Lambda}$ is the vector of the 16×16 generalized Gell-Mann matrices [24], whose first component represents identity matrix. Here, $i, j \in \{0, 1, 2, 3, ..., 255\}$ and Λ_i, Λ_j are $i, j-$th components of $\vec{\Lambda} = \left(\mathbb{I}, \; \Lambda_1, \; \Lambda_2, \; \Lambda_3, \; ..., \Lambda_{254}, \; \Lambda_{255} \right)$ respectively. Also $p_i^{(s)}$ and $q_j^{(t)}$ are real coefficients.

Then from the above relation (6) and using the actual form of the universal witness operator (5), the referee will calculate the quantities,

$$\mathrm{Tr}\big(W^{\mathrm{univ}}(\Lambda_i \otimes \Lambda_j)\big) = (16)^2 \sum_{s,t} \beta_{s,t} \; p_i^{(s)} \; q_j^{(t)},$$

that will give a set of $(256)^2$ number of linear equations for all i, j, from which the referee calculates the coefficients $\beta_{s,t}$ in equ. (6). Also, instead of using a two-qubit Bell state projector $|\phi^+\rangle \langle \phi^+| = \frac{1}{2} \sum_{i,j=0}^1 |ii\rangle \langle jj|$ or it's local unitary equivalent as a measurement operator, each party should use Bell state projector of two sixteen dimensional systems as the measurement operator $|\Phi^+\rangle \langle \Phi^+| = \frac{1}{16} \sum_{i,j=0}^{15} |ii\rangle \langle jj|$ or it's local unitary equivalent, for each party. Then the negativity of

$$I(\rho_{\mathcal{AB}}) = \det(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}) = \mathrm{Tr}\big[W^{\mathrm{univ}}(\rho_{\mathcal{A}_1\mathcal{B}_1} \otimes \rho_{\mathcal{A}_2\mathcal{B}_2} \otimes \rho_{\mathcal{A}_3\mathcal{B}_3} \otimes \rho_{\mathcal{A}_4\mathcal{B}_4})\big]$$

$$= \sum_{s,t} \beta_{s,t} \mathrm{Tr}\Big[\Big(|\Phi^+\rangle_{\mathcal{A}_0:\mathcal{A}_1\mathcal{A}_2\mathcal{A}_3\mathcal{A}_4} \langle \Phi^+| \otimes |\Phi^+\rangle_{\mathcal{B}_0:\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4} \langle \Phi^+|\Big) \Big(\tau_s^{(\mathcal{A}_0)} \otimes \rho_{\mathcal{A}_1\mathcal{B}_1} \otimes \rho_{\mathcal{A}_2\mathcal{B}_2} \otimes \rho_{\mathcal{A}_3\mathcal{B}_3} \otimes \rho_{\mathcal{A}_4\mathcal{B}_4} \otimes \omega_t^{(\mathcal{B}_0)}\Big)\Big] \qquad (8)$$

confirms the presence of entanglement of the shared state.

Here if we choose to work in the computational basis $\{|0\rangle, |1\rangle\}$, any pure state of a single party $\mathcal{A}$, can be written as,

$|\psi_{\mathcal{A}}\rangle = \big(\alpha |0\rangle_1 + \beta_1 |1\rangle\big)_{\mathcal{A}_1} \otimes \big(\alpha_2 |0\rangle + \beta_2 |1\rangle\big)_{\mathcal{A}_2} \otimes \big(\alpha_3 |0\rangle + \beta_3 |1\rangle\big)_{\mathcal{A}_3} \otimes \big(\alpha_4 |0\rangle + \beta_4 |1\rangle\big)_{\mathcal{A}_4}$,

such that the set $\{|\psi_{\mathcal{A}}\rangle, |\psi_{\mathcal{B}}\rangle\}$ spans the support of $\rho_{\mathcal{AB}}^{\otimes 4}$.

The form of the swap operators has to be found out by their action,

$$\tilde{V}^{(4)} |\psi_{\mathcal{A}}\rangle = \big(\alpha_4 |0\rangle + \beta_4 |1\rangle\big)_{\mathcal{A}_1} \otimes \big(\alpha_1 |0\rangle + \beta_1 |1\rangle\big)_{\mathcal{A}_2} \otimes \big(\alpha_2 |0\rangle + \beta_2 |1\rangle\big)_{\mathcal{A}_3} \otimes \big(\alpha_3 |0\rangle + \beta_3 |1\rangle\big)_{\mathcal{A}_4} \qquad (9)$$

Therefore,

$$\tilde{V}^{(4)} = \sum_{i,j,k,l=0}^1 |l, i, j, k\rangle \langle i, j, k, l| \quad \text{acts on } \mathcal{H}_{\mathcal{A}}^{\otimes 4} \qquad (10)$$

$$\tilde{V}^{(3)} \otimes \mathbb{I} |\psi_{\mathcal{A}}\rangle = \big(\alpha_3 |0\rangle + \beta_3 |1\rangle\big)_{\mathcal{A}_1} \otimes \big(\alpha_1 |0\rangle + \beta_1 |1\rangle\big)_{\mathcal{A}_2} \otimes \big(\alpha_2 |0\rangle + \beta_2 |1\rangle\big)_{\mathcal{A}_3} \otimes \big(\alpha_4 |0\rangle + \beta_4 |1\rangle\big)_{\mathcal{A}_4} \qquad (11)$$

Therefore,

$$\tilde{V}^{(3)} = \sum_{i,j,k=0}^1 |k, i, j\rangle \langle i, j, k| \quad \text{acts on} \quad \mathcal{H}_{\mathcal{A}}^{\otimes 3} \qquad (12)$$

Similar expressions are valid for the operaors act on $\mathcal{H}_{\mathcal{B}}^{\otimes n}$ where, $n = 3, 4$.

A general support vector in $\mathcal{H}_{\mathcal{AB}}{}^{\otimes 4}$ can be written as,

$$|\psi_{\mathcal{AB}}\rangle = \big(\alpha_1 |0\rangle + \beta_1 |1\rangle\big)_{\mathcal{A}_1} \otimes \big(\alpha'_1 |0\rangle + \beta'_1 |1\rangle\big)_{\mathcal{B}_1}$$
$$\otimes\big(\alpha_2 |0\rangle + \beta_2 |1\rangle\big)_{\mathcal{A}_2} \otimes \big(\alpha'_2 |0\rangle + \beta'_2 |1\rangle\big)_{\mathcal{B}_2}$$
$$\otimes\big(\alpha_3 |0\rangle + \beta_3 |1\rangle\big)_{\mathcal{A}_3} \otimes \big(\alpha'_3 |0\rangle + \beta'_3 |1\rangle\big)_{\mathcal{B}_3}$$
$$\otimes\big(\alpha_4 |0\rangle + \beta_4 |1\rangle\big)_{\mathcal{A}_4} \otimes \big(\alpha'_4 |0\rangle + \beta'_4 |1\rangle\big)_{\mathcal{B}_4} \quad (13)$$

Therefore,

$$V^{(2)} \otimes V^{(2)} |\psi_{\mathcal{AB}}\rangle$$
$$= \big(\alpha_2 |0\rangle + \beta_2 |1\rangle\big)_{\mathcal{A}_2} \otimes \big(\alpha'_2 |0\rangle + \beta'_2 |1\rangle\big)_{\mathcal{B}_2}$$
$$\otimes\big(\alpha_1 |0\rangle + \beta_1 |1\rangle\big)_{\mathcal{A}_1} \otimes \big(\alpha'_1 |0\rangle + \beta'_1 |1\rangle\big)_{\mathcal{B}_1}$$
$$\otimes\big(\alpha_4 |0\rangle + \beta_4 |1\rangle\big)_{\mathcal{A}_4} \otimes \big(\alpha'_4 |0\rangle + \beta'_4 |1\rangle\big)_{\mathcal{B}_4}$$
$$\otimes\big(\alpha_3 |0\rangle + \beta_3 |1\rangle\big)_{\mathcal{A}_3} \otimes \big(\alpha'_3 |0\rangle + \beta'_3 |1\rangle\big)_{\mathcal{B}_3} \quad (14)$$

Thus,

$$V^{(2)} = \sum_{i,j,k,l=0}^{1} |kl,ij\rangle \langle ij,kl| \quad \text{acts on} \ \ \mathcal{H}_{\mathcal{AB}}{}^{\otimes 2} \quad (15)$$

IV. UNIVERSAL WITNESS FOR NPT-NESS OF TWO-QUDIT STATES:

Any two-qudit density matrix which has at least one negative eigenvalue after partial transposition, is called an NPT state. Any bipartite state having NPT is necessarily entangled. Now, to determine NPT-ness of a unknown two-qudit state (i.e. to determine whether the state has NPT or PPT), we need to check negativity of the eigenvalues of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ [25]. Let us look at the characteristic equation for the matrix $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$:

$$\det(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}} - \lambda \mathbb{I}_{d^2 \times d^2}) = 0,$$

which is in the form, $\sum_{i=0}^{d^2}(-1)^{d^2-i} a_{d^2-i}\lambda^i = 0,$

$$(16)$$

where, the coefficients $a_0, a_1, a_2, ..., a_{d^2}$ can be given in terms of the eigenvalues $\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{d^2}$ of $\rho_{\mathcal{AB}}$ as follows :

$$a_0 = 1, a_1 = \sum_{i=1}^{d^2} \lambda_i, a_2 = \sum_{i,j=1;i>j}^{d^2} \lambda_i \lambda_j,$$

$$a_3 = \sum_{i,j,k=1;i>j>k}^{d^2} \lambda_i \lambda_j \lambda_k, ..., a_{d^2} = \prod_{i=1}^{d^2} \lambda_i$$

As $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ is hermitian, λ's are all real, and thereby a_i's are all real. If $a_i \geq 0 \ \forall \ i$, we have $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}} \geq 0$. Otherwise $\rho_{\mathcal{AB}}$ has NPT. Now, we can determine whether negative roots of the characteristic equation exist. We

can write each of these coefficients as a polynomial in λs'(eigenvalues of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$) using the Newton-Girard formulae [18]. In fact we have : $a_1 = 1$ because partial transposition operation is trace preserving;

$$a_2 = \frac{1}{2}\Big(1 - \sum_{i=1}^{d^2} \lambda_i^2\Big) = \mathrm{Tr}(W_2 \rho_{\mathcal{AB}}^{\otimes 2}), \quad \text{with,}$$

$$W_2 = \frac{1}{2}\Big[\mathbb{I}_{d^4 \times d^4} - V^{(2)}\Big]; \quad (17)$$

$$a_3 = \frac{1}{6}\Big(1 - 3\sum_{i=1}^{d^2} \lambda_i^2 + 2\sum_{i=1}^{d^2} \lambda_i^3\Big) = \mathrm{Tr}(W_3 \rho_{\mathcal{AB}}^{\otimes 3}),$$

$$\text{with,} \ W_3 = \frac{1}{6}\Big[\ \mathbb{I}_{d^6 \times d^6} - 3 \ \mathbb{I}_{d^2 \times d^2} \ \otimes \ V^{(2)}$$
$$+ \ \tilde{V}^{(3)} \ \otimes \ \tilde{V}^{(3)T} + \tilde{V}^{(3)T} \ \otimes \ \tilde{V}^{(3)}\Big]; \quad (18)$$

and, $a_4 =$

$$\frac{1}{24}\Big(1 - 6\sum_{i=1}^{d^2}\lambda_i^2 + 3\Big(\sum_{i=1}^{d^2}\lambda_i^2\Big)^2 + 8\sum_{i=1}^{d^2}\lambda_i^3 - 6\sum_{i=1}^{d^2}\lambda_i^4\Big)$$
$$= \mathrm{Tr}\big(W_4 \rho_{\mathcal{AB}}^{\otimes 4}\big)$$

$$(19)$$

where W_4 has the same expression as that of W^{univ} in Equ. (5); so on and so forth.

Our argument starts from finding the signature of the coefficients a_i with $i \geq 2$. For most favourable case, a_2 may turn out to be negative and thereby $\rho_{\mathcal{AB}}$ has NPT. So, two copies of the shared state, $\rho_{\mathcal{AB}}$ is enough to determine NPT-ness while both the inputs τ_s and ω_t are density matrices on Hilbert space $(\mathbb{C}^d)^{\otimes 2}$. But for the general case, the players have to share 'i' number of copies of the state $\rho_{\mathcal{AB}}$ whenever referee wants to know the sign of the coefficient a_i. Also the dimension of the input states (τ_s and ω_t to be supplied by the referee) should increase accordingly. For the worst case, we have to go upto the coefficient a_{d^2} for which we need d^2 copies of $\rho_{\mathcal{AB}}$ and τ_s and ω_t will be density matrices on the Hilbert space $(\mathbb{C}^d)^{\otimes d^2}$. As, for any PPT state $\rho_{\mathcal{AB}}$, all of $\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{d^2}$ are non-negative, all the coefficients $a_2, a_3, ..., a_{d^2}$ are non-negative. So, the operators, $W_2, W_3, ..., W_{d^2}$ indeed work as witnessing NPT-ness of the state $\rho_{\mathcal{AB}}$.

Note that, these witness operators don't depend on the shared state $\rho_{\mathcal{AB}}$, and so, we can use the scheme similar to that described in section III to implement the measurement of these operator in measurement device independent way. A notable point is that, for two-qubit case, under partial transposition, the shared density matrix can have only one negative eigenvalue, if the state is entangled [16]. Thus for the case of two-qubits, the sign of the coefficient a_4 is enough to decide the NPT-ness, and thereby entanglement of the state as done in section III. We don't need to check the signs of the coefficients a_2, a_3. But for higher dimensions, that is not the case.

A. Comparison between our MDI scheme and the conventional state tomography :

In state-tomography, for a two-qudit system, we surely need, d^4-1 number of measurement settings, as the number of coefficients in any basis representation (like generalized Gell-Mann matrices Λ_n [26]) are $d^4 - 1$:

$$\rho_{d^2 \times d^2} = \frac{1}{d^4}\left[\mathbb{I} \otimes \mathbb{I} + \sum_{n=1}^{d^4-1} r_n \Lambda_n \right]. \qquad (20)$$

Coefficients $r_n \in \mathbb{R}$, can be obtained from the expectation value of observable $\Lambda_n : r_n = \text{Tr}\left[\rho_{d^2 \times d^2} \Lambda_n \right]$. Therefore, for each coefficient, atleast single copy of the state has to be used. In order to reconstruct the state, we need to know exact values of the coefficients, their signs only don't give the sufficient information. The erroneous numerical values of these coefficients lead to a wrongly estimated state, $\rho_{d^2 \times d^2}$. So, it is not easy to think of a scheme like mesurement device independent tomography for a two-qudit system.

But in our case, without going into any MDI scheme, to measure a_2 in Equ. (17), we have to measure the expectation value of a single observable $V^{(2)}$ only. For a_3 in Equ. (18), we need to measure, expectation values of two observables $\mathbb{I}_{d^2 \times d^2} \otimes V^{(2)}$, $\tilde{V}^{(3)} \otimes \tilde{V}^{(3)T} + \tilde{V}^{(3)T} \otimes \tilde{V}^{(3)}$. Similarly for a_4, we have four observables to measure. So, we need very less number of measurement settings compared to the tomography, at the cost of $n-$copy usage for coefficient a_n.

In the universal MDI scheme of finding NPT-ness of any two-qudit state, for the coefficient a_n, we need two general Bell state projectors in Hilbert space $\mathbb{C}^{d^n} \otimes \mathbb{C}^{d^n}$, and the input density matrices τ_s, ω_t on Hilbert space $\mathbb{C}^{n^2}$. These inputs will span the vector space of W_n, so, their required number will depend on the number of observables in the expression of W_n, which is in general less than the observable in conventional tomography. For our case, the sign of the coefficients a_n's are enough to decide whether the shared state ρ_{AB} is entangled or separable.

V. WITNESSING AN ARBITRARY PPT ENTANGLED STATE OF A GIVEN BIPARTITE SYSTEM:

Existence of PPT entangled state ρ_{AB} (so called PPT bound entangled states) is well-known whenever $\dim(\mathcal{H}_A) \times \dim(\mathcal{H}_B) > 6$. Evidently our scheme of universal NPT-ness witness, as described in section IV, does not work here to detect entanglement of any such state. Below we try to argue that a universal entanglement witness operator can not exist to single out entanglement in any PPT state of a given bipartite sytem, through some conjectures.

Conjecture I : If $\dim(\mathcal{H}_A) \times \dim(\mathcal{H}_B) > 6$, there can not exist one (or a finitely many) universal entanglement
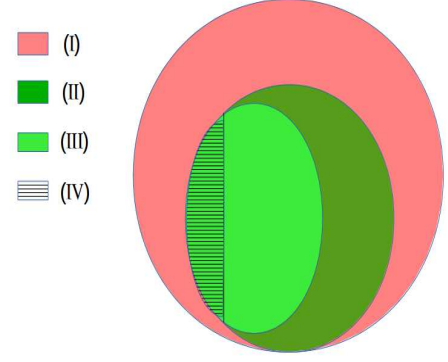

FIG. 2: (colour online) Distribution of density matrix spaces on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. [(I) + (II) + (III) + (IV)] $\equiv \mathcal{D}_{AB}$, the set of all density matrices. (I) $\equiv \mathcal{D}_{AB} - \mathcal{P}_{AB}$ is the set of all NPT states, $\mathcal{P}_{AB}$ is the set of all states having PPT (II) $\equiv \tilde{\mathcal{P}}_{AB}$ is the set of all PPT entangled states, [(III) + (IV)] $\equiv \mathcal{S}_{AB}$ is the set of all separable states, [(II) + (III)] $\equiv \tilde{\mathcal{P}}'_{AB}$ is the set of convex combination of PPT entangled states. Region (III) clearly depicts the non-empty-ness of $(\tilde{\mathcal{P}}'_{AB} \bigcap \mathcal{S}_{AB})$.

witness operator detecting entanglement in an arbitrary PPT state ρ_{AB}, and which can be realized in a MDI way.

Reason behind this conjecture is another conjecture,

Conjecture II : There can not exist a universal EW (or, a finitely many EW operators) for all PPT entangled states of any given bipartite system

Let us try to provide some geometrical argument which potentially may give rise to Conjecture II.

Let $\mathcal{D}_{AB}$, $\mathcal{S}_{AB}$, $\mathcal{P}_{AB}$ are respectively be the set of density matrices, separable density matrices, density matrices which are positive semidefinite under partial transposition (PPT), on $\mathcal{H}_{AB}$; $\tilde{\mathcal{P}}_{AB}$ be the set of all entangled density matrices (PPTE) in $\mathcal{P}_{AB}$. $\mathcal{S}_{AB}$ and $\mathcal{P}_{AB}$ are both convex sets. It is obvious that, $\mathcal{S}_{AB} \subset \mathcal{P}_{AB} \subset \mathcal{D}_{AB}$ and $\mathcal{P}_{AB} - \mathcal{S}_{AB} = \tilde{\mathcal{P}}_{AB}$. Note that $\tilde{\mathcal{P}}_{AB}$ is not convex. For $\max\{dim(\mathcal{H}_A), dim(\mathcal{H}_B)\} = 3$ together with $\min\{dim(\mathcal{H}_A), dim(\mathcal{H}_B)\} = 2$, $\mathcal{P}_{AB} = \mathcal{S}_{AB}$. Let $\tilde{\mathcal{P}}'_{AB}$ is the set of states formed by the convex combination of states $\in \tilde{\mathcal{P}}_{AB}$.

Edge state : $\rho_{AB} \in \tilde{\mathcal{P}}_{AB}$ is an edge state iff the state $(\rho_{AB} + p\sigma_{AB})/(1 + p) \in \mathcal{S}_{AB}$ for all $p \in (0, 1]$ and all $\sigma_{AB} \in \mathcal{S}_{AB}$. Edge states lie near the boundary of $\mathcal{S}_{AB}$ and exist for all $\dim(\mathcal{H}_A, \mathcal{H}_B) \geq 3$.

It is well known that [27, 28] there always exist atleast two edge states $\rho_{AB}^{(\alpha)}, \rho_{AB}^{(\beta)} \in \tilde{\mathcal{P}}_{AB}$ such that, their convex combination, $p\rho_{AB}^{(\alpha)} + (1 - p)\rho_{AB}^{(\beta)} = \sigma_{AB} \in \mathcal{S}_{AB}$ for $0 \leq p \leq 1$. Hence for, $dim(\mathcal{H}_A), dim(\mathcal{H}_B) \geq 3$, $\tilde{\mathcal{P}}'_{AB} \cap \mathcal{S}_{AB} \neq \phi$ (null set). This is the case for single copy. Fig.2 depicts existence of these edge states in region (II) near the boundary of (II) and (III).

From Fig.2 it is clear that, there can not exist a hermitian operator $W : \mathbb{C}^d \otimes \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$ such that

$\text{Tr}[W\rho_{\mathcal{AB}}] < 0$ for all $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ while $\text{Tr}[W\sigma_{\mathcal{AB}}] \geq 0$ for all $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$. So, in the single copy case no such universal witness operator W exists to witness entanglement in every $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$.

Now, the question is — As in the case of qubits, is it possible to have a (for finite number of) universal witness operator(s) W^{univ} which can detect entanglement in any PPT state $\rho_{\mathcal{AB}}$ of two-qudits in case $n-$copies of the state are supplied with $n \geq 2$?

We conjecture that, such a W^{univ} does not exist.

Let's consider, $\mathcal{D}_{\mathcal{A}_n\mathcal{B}_n}$ is the set of all density matrices in $\mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$. $\mathcal{S}'_{\mathcal{AB}}{}^{(n)}$ is the set formed by the convex combination of the states $\sigma_{\mathcal{AB}}^{\otimes n}$, where, $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$ and $\tilde{\mathcal{P}}'_{\mathcal{AB}}{}^{(n)}$ is the set formed by the convex combination of the states $\rho_{\mathcal{AB}}^{\otimes n}$, where, $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$. If $\mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ be the set of all separable states in $\mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$, it is evident that, $\mathcal{S}'_{\mathcal{AB}}{}^{(n)} \in \mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ and it is most likely that, $\mathcal{S}_{\mathcal{A}_n\mathcal{B}_n} \cap \tilde{\mathcal{P}}'_{\mathcal{AB}}{}^{(n)} \neq \phi$ (null set), for all n with $dim(\mathcal{H}_{\mathcal{A}}), dim(\mathcal{H}_{\mathcal{B}}) \geq 3$, because of the existence of edge states in $\mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$.

Conjecture III: $\mathcal{S}'_{\mathcal{AB}}{}^{(n)} \cap \tilde{\mathcal{P}}'_{\mathcal{AB}}{}^{(n)} \neq \phi$ (null set) for all n with $dim(\mathcal{H}_{\mathcal{A}}), dim(\mathcal{H}_{\mathcal{B}}) \geq 3$.

Fig.2 depicts Conjecture III is true for $n = 1$.

That means, there always exist atleast two states $\rho_{\mathcal{AB}}^{(\alpha)}, \rho_{\mathcal{AB}}^{(\beta)} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ such that, the convex combination of their n number of copies,

$$p(\rho_{\mathcal{AB}}^{(\alpha)})^{\otimes n} + (1 - p)(\rho_{\mathcal{AB}}^{(\beta)})^{\otimes n} = \sum_r p_r (\sigma_{\mathcal{AB}}^{(r)})^{\otimes n} \quad (21)$$

is a density matrix describes a separable state $\in \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$, $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$, and this holds for any $n \in \mathbb{N}$.

Where $\mathbb{N}$ is the set of all natural numbers, $0 \leq p_r \leq 1$ forall r and $\sum_r p_r = 1$.

Validity of conjecture III implies nonexistence of any hermitian operator,

$$W_{\mathcal{A}_n\mathcal{B}_n} : \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n} \to \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n},$$

for which, $\text{Tr}[W_{\mathcal{A}_n\mathcal{B}_n}(\rho_{\mathcal{AB}})^{\otimes n}] < 0$ for *some* $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ together with $\text{Tr}[W_{\mathcal{A}_n\mathcal{B}_n}(\sigma_{\mathcal{AB}})^{\otimes n}] \geq 0$ for *all* $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$ — irrespective of the choice of n.

Thus, validity of conjecture III implies that there can not exist a universal EW (or, a finitely many EWs) which can detect entanglement in all the PPT (bound) entangled states of $\mathcal{A} + \mathcal{B}$ whenever $d \geq 3$.

This atomatically implies the validity of the conjecture II. It appears to be quite difficult to verify conjecture III directly. One may try to verify whether for some given states $\rho_{\mathcal{AB}}^{\alpha} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$, there exist a separable state, $\sigma_{\mathcal{AB}} \in \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$ such that,

$$\text{Tr}\Big[\mathcal{O} \sum_\alpha p_\alpha (\rho_{\mathcal{AB}}^{(\alpha)})^{\otimes n}\Big] = \text{Tr}\Big[\mathcal{O} \, \sigma_{\mathcal{AB}}\Big],$$
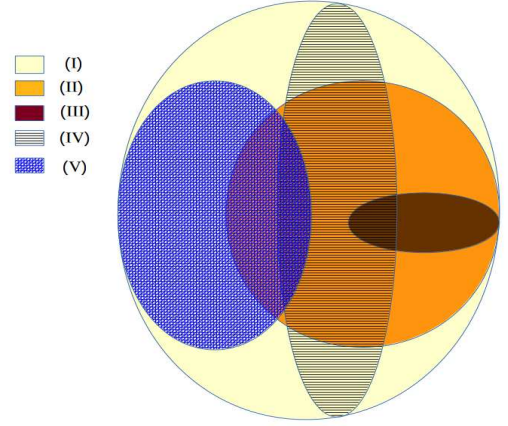

FIG. 3: (colour online) Distribution of density matrix spaces on Hilbert space $\mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$. [(I) $\bigcup$ (II) $\bigcup$ (III) $\bigcup$ (IV) $\bigcup$ (V)] $\equiv \mathcal{D}_{\mathcal{A}_n\mathcal{B}_n}$, the set of all density matrices. (II)$\equiv \mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ is the set of all separable states, (III) $\equiv \mathcal{S}'_{\mathcal{AB}}{}^{(n)}$ is the set of convex combinations of all states like $\sigma_{\mathcal{AB}}^{\otimes n}$, where $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$. (IV) $\equiv \tilde{\mathcal{P}}'_{\mathcal{AB}}{}^{(n)}$ is the convex combination of the states like $\rho_{\mathcal{AB}}^{\otimes n}$, where $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$. (V) contains convex combination of all the states like $\rho_{\mathcal{AB}}^{\otimes n}$, where $\rho_{\mathcal{AB}} \in \mathcal{D}_{\mathcal{AB}} - \tilde{\mathcal{P}}_{\mathcal{AB}}$, set of all NPT states at the single copy level. We conjecture about the non-emptyness of the intersection (III) $\bigcap$ (IV), and the empty-ness of, (III) $\bigcap$ (V) = ϕ (null set).

for a complete set of linearly independent observables $\mathcal{O} : \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n} \to \mathcal{H}_{\mathcal{A}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes n}$. Even verification of this one may turn out to be difficult.

This difficulty seems to arise from the well-known fact that the separability problem (that is to find out whether *arbitrary* state of a given bipartite quantum system is entangled or separable) is NP-hard [29, 30] .

VI. NOISE ANALYSIS FOR REAL EXPERIMENTS :

Recently, a few experimental works [13, 31] have been done to implement this MDI protocol to test the entanglement of two particular type of two-qubit states.

We now analyse the effect of possible noises in the Bell-state-measurement (BSM) part of their experimental setups. Here we introduce three kinds of possible noise (see Fig. 4) :

(1) Photon loss in the polarizing beam splitter (PBS) : We model here the photon loss in a PBS through the action of a white noise - as described below.

(2) Error in the angle of rotation in the half wave plate (HWP) : HWP rotates the polarization axis of the light vector (which carries the information about the projected state by the measurement operator) with respect to it's direction of the propagation of light ray by the angle equals two times of the angle (θ) between the fast axis of HWP and the polarization axis. So, if the
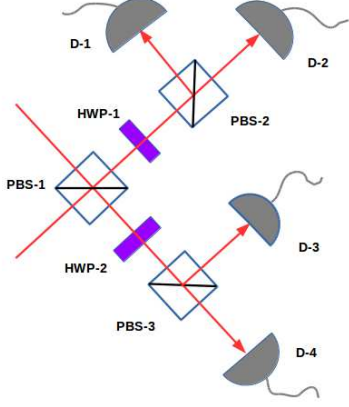
FIG. 4: (colour online) Bell-state projection $\frac{1}{2}(|HH\rangle + VV)(\langle HH| + \langle VV|)$ measurement via coincidence counts. Photon propagations are denoted by red-rays.
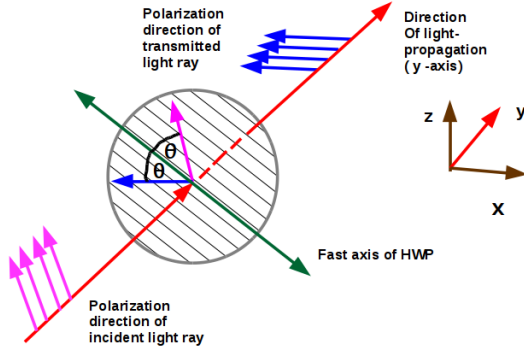

FIG. 5: (colour online) Light ray passing through Half wave plate. The polarization axis, rotates by angle 2θ with respect to the direction of propagation. θ is the angle between the fast axis of the direction of polarization of the incident light ray. The first axis of the HWP lies in the $xz-$plane.

angle of rotation be improper, we can it as $2\theta + \eta$, where η is the error in BSM.

(3) Detection inefficiency in the PBS and Diode photon-detector parts : For detection inefficiency, the probability of detection sets reduced by a factor ξ such that $0 \leq \xi \leq 1$ and the probability of detection become $\xi P(1, 1|\tau_s, \omega_t)$.

For our discussion we have chosen $|\Phi^+\rangle \langle \Phi^+|$ a Bell state projector as measurement operator (as the projector of BSM), where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ with the consideration that the horizontally polarized state is $|H\rangle = (1 \quad 0)^T \equiv |0\rangle$ and vertically polarized state is $|V\rangle = (0 \quad 1)^T \equiv |1\rangle$.

Under additive white noise (a special case), our actual measurement operator will be, $\mu|\Phi^+\rangle \langle \Phi^+| + \frac{1-\mu}{4}\mathbb{I}$, where μ is the corresponding visibility.

We assume the direction of propagation of photon is along y axis (denoted by red rays in Fig. 4 and Fig. 5), where the reference coordinate frames fixed at every HWP. Thus if the angle of rotation for the polarization axis (shown in Fig. 5) of one player and that coming from the referee are respectively $2g_1$ and $2g_2$ then, **rotated**

$$|\Phi^+\rangle = e^{-ig_1\sigma_y} \otimes e^{-ig_2\sigma_y}|\Phi^+\rangle$$
$$= \cos(g_2 - g_1)|\Phi^+\rangle + \sin(g_2 - g_1)|\Psi^-\rangle \quad (22)$$

where, $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. So, if g_1 and g_2 are the same or $\pm\pi$ or $\pm 2\pi$ then there is no error in the HWP. Therefore after passing through noisy PBS and HWP, our noisy Bell state projector will be,

$$P = \mu \cos^2(g_2 - g_1)|\Phi^+\rangle \langle \Phi^+|$$
$$+\mu \cos(g_2 - g_1)\sin(g_2 - g_1)\Big(|\Psi^-\rangle \langle \Phi^+| + |\Phi^+\rangle \langle \Psi^-|\Big)$$
$$+\mu \sin^2(g_2 - g_1)|\Psi^-\rangle \langle \Psi^-| + \frac{1-\mu}{4}\mathbb{I} \quad (23)$$

Let's take $g_2 - g_1 = \Delta$. Then the noisy projection operator shared between $\mathcal{A}$ and a part come from the referee $\mathcal{A_O} =$

$$P_{\mathcal{A_O A}} = \mu_1 \cos^2(\Delta_1)|\Phi^+\rangle \langle \Phi^+|$$
$$+\mu_1 \cos(\Delta_1)\sin(\Delta_1)\Big(|\Psi^-\rangle \langle \Phi^+| + |\Phi^+\rangle \langle \Psi^-|\Big)$$
$$+\mu_1 \sin^2(\Delta_1)|\Psi^-\rangle \langle \Psi^-| + \frac{1-\mu_1}{4}\mathbb{I} \quad (24)$$

Similarly for $\mathcal{B}$ and $\mathcal{B_O}$,

$$P_{\mathcal{B B_O}} = \mu_2 \cos^2(\Delta_2)|\Phi^+\rangle \langle \Phi^+|$$
$$+\mu_2 \cos(\Delta_2)\sin(\Delta_2)\Big(|\Psi^-\rangle \langle \Phi^+| + |\Phi^+\rangle \langle \Psi^-|\Big)$$
$$+\mu_2 \sin^2(\Delta_2)|\Psi^-\rangle \langle \Psi^-| + \frac{1-\mu_2}{4}\mathbb{I} \quad (25)$$

Here, μ_1 and μ_2 are the visibilities of the PBS's of the party $\mathcal{A}-$ side and $\mathcal{B}-$side respectively in the noisy measurement of $|\Phi^+\rangle$. Δ_1 and Δ_2 are the corresponding errors in rotational angle in HWP in $\mathcal{A}-$ side and $\mathcal{B}-$side respectively.

So, our desired (modified) quantity will be,

$$I_{\text{mod}}(\rho_{\mathcal{AB}}) =$$
$$\sum_{s,t} \beta_{s,t} \, \xi \, \text{Tr}\Big[(P_{\mathcal{A_O A}} \otimes P_{\mathcal{B B_O}})(\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t)\Big]$$
$$= \xi\Big[\mu_1\mu_2 \cos^2(\Delta_1)\cos^2(\Delta_2) + \frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1)$$
$$+\frac{\mu_2(1-\mu_1)}{4}\cos^2(\Delta_2) + \frac{(1-\mu_1)(1-\mu_2)}{16}\Big]$$
$$I(\rho_{\mathcal{AB}}) + \text{additional term.} \quad (26)$$

The additional term is in Equ. (42) and (43) of appendix VII B.

Now, for simplicity, let us assume that $\mu_1 = \mu_2 = \mu$ and $\Delta_1 = \Delta_2 = \Delta$.

In the case of a two-qubit shared state $\rho_{\mathcal{AB}}$, the input states τ_s and ω_t takes the forms,

$$\tau_s = \frac{\mathbb{I} + \vec{r}_s.\vec{\sigma}}{2}, \quad \omega_t = \frac{\mathbb{I} + \vec{r}_t.\vec{\sigma}}{2}, \quad \rho_{\mathcal{AB}} = \frac{1}{4}\Big(\mathbb{I} \otimes \mathbb{I} + \sum_{i=1}^{3} a_i \ \mathbb{I} \otimes \sigma_i + \sum_{i=1}^{3} b_i \ \sigma_i \otimes \mathbb{I} + \sum_{i,j=1}^{3} c_{ij} \ \sigma_i \otimes \sigma_j\Big) \qquad (27)$$

$$\text{with,} \quad \vec{r}_{s,t} = (x_{s,t}, \ y_{s,t}, \ z_{s,t}) \in \mathbb{R}^3, \ |\vec{r}_{s,t}| \leq 1, \ (a_1, a_2, a_3) \in \mathbb{R}^3, \ (b_1, b_2, b_3) \in \mathbb{R}^3$$
$$\text{and } (c_{ij})_{i,j=1}^{3} \text{ is a real } 3 \times 3 \text{ matrix.}$$

The corresponding form of $I_{\mathrm{mod}}(\rho_{\mathcal{AB}})$ is given in, appendix [VII B]

According to ref. [31], the input states are given in table -I,

Input states τ_s, ω_t	Bloch vectors $\vec{r}_s, \vec{r}_t$
$|H\rangle\langle H|$	(0, 0, 1)
$|V\rangle\langle V|$	(0, 0,-1)
$|D\rangle\langle D|$	(1, 0, 0)
$|\bar{D}\rangle\langle\bar{D}|$	(-1, 0, 0)
$|L\rangle\langle L|$	(0, 1, 0)
$|R\rangle\langle R|$	(0,-1, 0)

Table - I : Input states used in the ref. [31] for Alice and Bob's side and their corresponding bloch vectors.

The corresponding payoffs are :

$$\beta_{H,H} = \beta_{V,V} = \beta_{D,D} = \beta_{\bar{D},\bar{D}} = \beta_{L,L} = \beta_{R,R} = \frac{1}{3},$$
$$\beta_{H,V} = \beta_{V,H} = \beta_{D,\bar{D}} = \beta_{\bar{D},D} = \beta_{L,R} = \beta_{R,L} = -\frac{1}{6}. \tag{28}$$

Other $\beta_{s,t}$ are equal to zero.

The shared state is, $\rho_{\mathcal{AB}} = p\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{4}\,\mathbb{I}$ which is separable iff $0 \leq p \leq \frac{1}{3}$. Thus in Equ. (27), $c_{11} = c_{22} = c_{33} = -p$. $c_{kl} = 0$; when $k \neq l$; $a_k = b_k = 0$ $\forall k,l \in \{1,2,3\}$.

Using Equ. (28) and table-I we have,

$$\sum_{s,t}\beta_{s,t} = 1,$$
$$\sum_{s,t}\beta_{s,t} \ x_s x_t = \sum_{s,t}\beta_{s,t} \ y_s y_t = \sum_{s,t}\beta_{s,t} \ z_s z_t = 1,$$
$$\sum_{s,t}\beta_{s,t}x_s y_t = \sum_{s,t}\beta_{s,t}x_s z_t = \sum_{s,t}\beta_{s,t}y_s x_t$$
$$= \sum_{s,t}\beta_{s,t}y_s z_t = \sum_{s,t}\beta_{s,t}z_s x_t = \sum_{s,t}\beta_{s,t}z_s y_t = 0. \tag{29}$$

Therefore, according to Equ. (26) (see Equ. (44) in Appendix VII B),

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \frac{\xi}{4}\big[1 - p\mu^2 - 2p\mu^2 \cos(4\Delta)\big] \tag{30}$$

For the allowed values of the noise parameters ξ, μ, Δ we have, $0 \leq I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) \leq \frac{1}{3}$. Hence for these kinds of errors no separable state will never be detected as entangled state.

Ref. [13] deals with the entangled state, $\rho = (1 - r)\,|\Psi^-\rangle\langle\Psi^-| + \frac{r}{2}(|HH\rangle\langle HH| + |VV\rangle\langle VV|)$ with $0 \leq r \leq 1$. $\rho_{\mathcal{AB}}$ is separable for $\frac{1}{2} \leq r \leq 1$. Here, for this case, $c_{11} = c_{22} = (r-1)$ and $c_{33} = 2r-1$. $c_{kl} = 0$; when $k \neq l$; $a_k = b_k = 0, \forall k,l \in \{1,2,3\}$.

Here we are going to use the data of the Table II of the Supplementary section of ref. [13].

for that case,

$$\sum_{s,t}\beta_{s,t} = 1,$$
$$\sum_{s,t}\beta_{s,t}x_s x_t = \sum_{s,t}\beta_{s,t}y_s y_t = 1, \sum_{s,t}\beta_{s,t}z_s z_t = 1,$$
$$\sum_{s,t}\beta_{s,t}z_s x_t = \sum_{s,t}\beta_{s,t}z_s y_t = \sum_{s,t}\beta_{s,t}x_s y_t =$$
$$\sum_{s,t}\beta_{s,t}x_s z_t = \sum_{s,t}\beta_{s,t}y_s x_t = \sum_{s,t}\beta_{s,t}y_s z_t = 0,$$
$$\tag{31}$$

Therefore, according to Equ. (26),   (see Equ. (44) in Appendix VII B),

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \frac{\xi}{4}[(3r-2)\mu^2 \cos(4\Delta) + \mu^2(r-1) + 1]. \tag{32}$$

For $\frac{1}{2} \leq r \leq 1$ and for allowed values of noise parameters ξ, μ, Δ, we have $0 \leq I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) \leq \frac{1}{2}$. So, as in the case of Ref. [31], separable states will never detected as entangled.

VII. CONCLUSION:

Using the prescription of Auguisiak et al. [16] for witnessing entanglement in a unknown state of two-qubits, we have extended here the measurement device independent entanglement witness scheme of Branciard et al. [14] to a universal measurement device independent entanglement witness scheme for two-qubit states, the caveat being that we need four copies of the state at a time and the referee should supply the input statesfrom sixteen dimension Hilbert spaces of Alice and Bob. In an aim to extend this result to higher dimension, we provided here a measurement device independent scheme for universally witnessing NPT-ness of a unknown state of any given bipartite system - provided many copies of the state is being supplied. Of course, that number of copies is much less than that required for state tomography. We conjectured that, there doesn't exist a single or a finite number of universal witness operators for witnessing entanglement in an arbitrary PPT state of a given bipartite system. Our noise analysis of the Bell state measurement scenario in both the experimental demonstration of MDIEW [13, 31] are in conformity with the MDI of EW of Branciard et al. [14].

[1] A. K. Ekert *Phys. Rev. Lett.* **67**, 661 (1991)
[2] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger *Nature*, **390**, 575-579 (1997)
[3] L. Maccone, *Phys. Rev. A*, **88**, 042109 (2013)
[4] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal *Phys. Rev. Lett.* **83**, 3081 (1999)
[5] C. H. Bennett and S. J. Wiesner *Phys. Rev. Lett.* **69**, 2881 (1992)
[6] R. Jozsa *arxiv.org/pdf/quant-ph/9707034*, (1997)
[7] A.Peres *Phys. Rev. Lett.* **77**,1413(1996)
[8] R. Horodecki and M. Horodecki *Phys. Rev. A* **54**, 1838 (1996)
[9] L. M. Ioannou, B. C. Travaglione, D. Cheung, and A. K. Ekert *Phys. Rev. A* **70**, 060303(R), (2004)
[10] L. M. Ioannou and B. C. Travaglione *Phys. Rev. A* **73**, 052314 (2006)
[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki *Rev.Mod.Phys.* **81** ,865 (2009)
[12] R. Augusiak,J. Bae,J. Tura and M. Lewenstein *J. Phys. A:Math.Theor* **47** 065301(2014)
[13] P. Xu, X. Yuan, L.K. Chen, He Lu, X.C. Yao, X. Ma, Yu-Ao Chen, and J.W. Pan *Phys. Rev. Lett* **112** ,140506(2014)
[14] C. Branciard, D. Rosset, Y.C. Liang, and N. Gisin *Phys. Rev. Lett.* **110**, 060405 (2013)
[15] F.Buscemi *Phys. Rev. Lett.* **108** 200401(2012).
[16] R. Augusiak, M. Demianowicz and P. Horodecki *Phys. Rev. A.* **77**, 030301 (2008)
[17] M. Horodecki, P. Horodecki, R. Horodecki *Physics Letters A* **223**, 1-8 (1996)
[18] D. G. Mead *The American Mathematical Monthly* **99**, 749-751 (1992)
[19] P. Horodecki *Phys. Rev. A.* **68** ,052101(2003)
[20] A. K. Ekert, C. Moura Alves, D. K. L. Oi, M. Horodecki, P. Horodecki and L. C. Kwek *Phys. Rev. Lett.* **88** , 217901 (2002)
[21] K. Bartkiewicz,P. Horodecki,K. Lemr, A. Miranowicz and K. Zyczkowski *Phys Rev A.* **91** , 032315(2015)
[22] Xiao Yuan, Quanxin Mei, Shan Zhou, and Xiongfeng Ma, *Phys. Rev. A* **93**, 042317 (2016)
[23] E. Verbanis, A. Martin, D. Rosset, C.C.W. Lim, R.T. Thew, and H. Zbinden, *Phys. Rev. Lett.* **116**, 190501 (2016)
[24] G. Kimura *Physics Letters A* **314**, 339349 (2003)
[25] P. Horodecki,A. Ekert *Phys. Rev. Lett.* **89**, 127902(2002)
[26] Reinhold A Bertlmann and Philipp Krammer, *J. Phys. A: Math.Theor.* **41** 235303 (2008)
[27] S. Bandyopadhyay, S. Ghosh, and V. Roychowdhury *Phys. Rev. A* **77**, 032318(2008)
[28] R. Augusiak, J. Grabowski, M. Kus, M. Lewenstein, *Optics Communications* **283** 805813 (2010)
[29] L. Gurvits, *Journal of Computer and System Sciences* **69** 448 484 (2004)
[30] S. Gharibian *Quantum Information and Computation*, **10**, 343-360, (2010)
[31] M. Nawareg, S. Muhammad, E. Amselem and M. Bourennane *Scientific Reports* **5**, 8048 (2015)

APPENDIX

A.   Inputs and measurement operators are noisy

An usual apparatus is generally influenced by ambient noise. In [14], the players and referee trust the preparation of the input states. So, the noise in τ_s and ω_t (if any), is supposed to be known by the referee (or, even by the players). Some noise may affect the actual shared state $\rho_{\mathcal{AB}}$, but as we are going to detect it, we will consider the noise induced shared state as the actual state $\rho_{\mathcal{AB}}$, need to be detected.

Any general $d-$dimensional noise can be expressed as $\frac{1}{d}\vec{n}.\vec{\Lambda}_{d\times d}$ where n^i and Λ^i are the ith components of generalized Bloch vector and Gell-Mann matrix in d-dimension respectively, $\Lambda^0 = \mathbb{I}_{d\times d}$ [26]. If the visibility μ of the actual input

state is same for all input states, and assume the visibility remains constant throughout the experiment, then the players (Alice and Bob) would receive the input states,

$$\tau'_s = \mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1.\vec{\Lambda}_{d\times d} = \left[\frac{(1-\mu)}{d}\vec{n}_1 + \frac{\mu}{d}\text{Tr}(\tau_s\vec{\Lambda}_{d\times d})\right].\vec{\Lambda}_{d\times d}, \text{ and } \quad \omega'_t = \left[\frac{(1-\mu)}{d}\vec{n}_2 + \frac{\mu}{d}\text{Tr}(\omega_t\vec{\Lambda}_{d\times d})\right].\vec{\Lambda}_{d\times d}$$

instead of τ_s and ω_t respectively . If the referee does not aware about the noise mixed with the inputs, there will be mismatch of the value of $\mathcal{I}(\rho_{A\mathcal{B}})$ from it's actual value if the refree knows the noise.

In the game, the form of W is known to the referee, he calculates the pay-off functions, $\beta_{s,t}$ according to the inputs [2]. If referee uses τ_s and ω_t as the inputs instead of τ'_s and ω'_t, his calculated $\beta_{s,t}$ will be different than the actual that will give the actual value of $I(\rho_{A\mathcal{B}})$.

Modified witness operator looks like,

$$W' = \sum_{s,t} \beta_{s,t}\tau'^T_s \otimes \omega'^T_t = \frac{\mu^2}{d^2}\sum_{s,t}\beta_{s,t}\tau^T_s \otimes \omega^T_t + \quad \text{additional noise terms.} \tag{33}$$

So, by knowing the amount of noise induced in inputs, referee can calculate the modified value of $\beta_{s,t}$, which comes from the linear equation generated by, $\text{Tr}[W'(\tau'^T_s \otimes \omega'^T_t)]$, for all s, t.

So, we can claim that if the referee knows about the character of the noise in inputs, entanglement determination shouldn't be erroneous.

In general, the measurement operators can also noisy, and the character of the noise is not supposed to be known by the referee nor by the players. But that noise can obviously affect the final decision based on the value of $I(\rho_{A\mathcal{B}})$. If a general additive noise, $\frac{1}{d^2}\vec{m}.\vec{\Lambda}_{d^2\times d^2}$ is added with the maximally entangled projector $\frac{1}{d}\sum_{i,j=1}^{d}|ii\rangle\langle jj|$, then with the visibility ν of the original measurement operator, the actual measurement operator appears as

$$\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}.\vec{\Lambda}_{d^2\times d^2},$$

provided this is a positive operator, that is $\forall\ |\chi\rangle$ we have,

$$\langle\chi|\left(\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}.\vec{\Lambda}_{d^2\times d^2}\right)|\chi\rangle \geq 0,$$

In the standard basis,$\{|i,j\rangle\}$, we can write

$$\vec{\Lambda}_{d^2\times d^2} = \sum_{a,b,p,q}\langle a,b|\vec{\Lambda}|p,q\rangle |a,b\rangle\langle p,q|$$

For notational convenience, in place of $\rho_{A\mathcal{B}}$, we will be using ρ here and also Λ for $\Lambda_{d^2\times d^2}$.

$$P_\rho(1,1|s,t) = \text{Tr}\left[\left\{\left(\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}_1.\vec{\Lambda}\right) \otimes \left(\frac{\nu}{d}\sum_{u,v}|uu\rangle\langle vv| + \frac{(1-\nu)}{d^2}\vec{m}_2.\vec{\Lambda}\right)\right\}\left(\tau_s \otimes \rho \otimes \omega_t\right)\right]$$

$$= \frac{\nu^2}{d^2}\text{Tr}\left[\left(\tau^T_s \otimes \omega^T_t\right)\rho\right] + \frac{\nu(1-\nu)}{d^3}\text{Tr}\left[\left(\tau^T_s \otimes \text{Tr}_{\mathcal{B}_\mathcal{O}}[(\vec{m}_2.\vec{\Lambda})(\mathbb{I}\otimes\omega_t)]\right)\rho\right]$$

$$+ \frac{\nu(1-\nu)}{d^3}\text{Tr}\left[\left(\text{Tr}_{\mathcal{A}_\mathcal{O}}[(\tau_s\otimes\mathbb{I})(\vec{m}_1.\vec{\Lambda})] \otimes \omega^T_t\right)\rho\right] + \frac{(1-\nu)^2}{d^4}\text{Tr}\left[\left(\text{Tr}_{\mathcal{A}_\mathcal{O}}[(\tau_s\otimes\mathbb{I})\vec{m}_1.\vec{\Lambda}] \otimes \text{Tr}_{\mathcal{B}_\mathcal{O}}[\vec{m}_2.\vec{\Lambda}(\mathbb{I}\otimes\omega_t)]\right)\rho\right]$$

$$= \frac{1}{d^2}\text{Tr}\left[\tau''^T_s \otimes \omega''^T_t \rho\right]. \tag{34}$$

If in (34) $\vec{m}_1.\vec{\Lambda} = \vec{m}_2.\vec{\Lambda} = \mathbb{I}_{d\otimes d} \otimes \mathbb{I}_{d\otimes d}$, will be denoted here as $\mathbb{I} \otimes \mathbb{I}$, and if define $\vec{\Lambda} = (\mathbb{I}, \vec{\Gamma})$, then

$$\tau_s^{''T} \otimes \omega_t^{''T} \quad = \quad \frac{\nu^2}{d^2}\tau_s^T \otimes \omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T \otimes tr_{\mathcal{B}_\mathcal{O}}\left[(\mathbb{I} \otimes \mathbb{I})(\mathbb{I} \otimes \omega_t)\right]$$

$$+\frac{\nu(1-\nu)}{d^3}tr_{\mathcal{A}_\mathcal{O}}\left[(\tau_s \otimes \mathbb{I})(\mathbb{I} \otimes \mathbb{I})\right] \otimes \omega_t^T + \frac{(1-\nu)^2}{d^4}tr_{\mathcal{A}_\mathcal{O}}\left[(\tau_s \otimes \mathbb{I})\mathbb{I} \otimes \mathbb{I}\right] \otimes \mathrm{Tr}_{\mathcal{B}_\mathcal{O}}\left[\mathbb{I} \otimes \mathbb{I}(\mathbb{I} \otimes \omega_t)\right]$$

$$=\frac{\nu^2}{d^2}\tau_s^T \otimes \omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T \otimes \mathbb{I} + \frac{\nu(1-\nu)}{d^3}\mathbb{I} \otimes \omega_t^T + \frac{(1-\nu)^2}{d^4}\mathbb{I} \otimes \mathbb{I}$$

$$=\frac{1}{d^4}\mathbb{I} \otimes \mathbb{I} + \frac{\nu}{d^4}\left(\mathbb{I} \otimes \vec{\Gamma}\right).tr(\vec{\Gamma}\omega_t^T) + \frac{\nu}{d^4}\left(\vec{\Gamma} \otimes \mathbb{I}\right).tr(\vec{\Gamma}\tau_s^T) + \frac{\nu^2}{d^4}\left(\vec{\Gamma}.tr(\vec{\Gamma}\tau_s^T)\right) \otimes \left(\vec{\Gamma}.tr(\vec{\Gamma}\omega_t^T)\right)$$

$$=\frac{1}{d^4}\left(\mathbb{I} + \nu\vec{\Gamma}.tr(\vec{\Gamma}\tau_s^T)\right)\left(\mathbb{I} + \nu\vec{\Gamma}.tr(\vec{\Gamma}\omega_t^T)\right) \tag{35}$$

Thus this is just a shrinking operation of the generalized Bloch vector $\vec{\Gamma}$.

If the referee is unaware about the noise then, there is deviation from the actual results.So, referee will use the β functions same as that obtained without noise.In presence of noise in inputs and measurement operator,the witness operator form becomes,

$$\sum_{s,t}\beta_{s,t}\left[\frac{\nu^2}{d^2}\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n_1}.\vec{\Lambda}_{d\times d}\right)^T \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n_2}.\vec{\Lambda}_{d\times d}\right)^T\right.$$

$$+\frac{\nu(1-\nu)}{d^3}\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1.\vec{\Lambda}_{d\times d}\right)^T \otimes tr_{\mathcal{B}_\mathcal{O}}\left[(\vec{m_2}.\vec{\Lambda})(\mathbb{I} \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2.\vec{\Lambda}_{d\times d}\right))\right]$$

$$+\frac{\nu(1-\nu)}{d^3}tr_{\mathcal{A}_\mathcal{O}}\left[\left(\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1.\vec{\Lambda}_{d\times d}\right) \otimes \mathbb{I}\right)(\vec{m}_1.\vec{\Lambda})\right] \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2.\vec{\Lambda}_{d\times d}\right)^T$$

$$+\frac{(1-\nu)^2}{d^4}\left\{tr_{\mathcal{A}_\mathcal{O}}\left[\left(\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1.\vec{\Lambda}_{d\times d}\right) \otimes \mathbb{I}\right)\vec{m}_1.\vec{\Lambda}\right] \otimes tr_{\mathcal{B}_\mathcal{O}}\left[\vec{m}_2.\vec{\Lambda}(\mathbb{I} \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2.\vec{\Lambda}_{d\times d}\right))\right]\right\}\right] \equiv W''(\text{say}) \tag{36}$$

.

Therefore, to get the correct result, in the expression of W, given by the equation [2], instead of $\tau_s^T \otimes \omega_t^T$ referee should use

$$\tau_s^{''T} \otimes \omega_t^{''T} = \frac{\nu^2}{d^2}\tau_s^T \otimes \omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T \otimes \mathrm{Tr}_{\mathcal{B}_\mathcal{O}}\left[(\vec{m_2}.\vec{\Lambda})(\mathbb{I} \otimes \omega_t)\right]$$

$$+\frac{\nu(1-\nu)}{d^3}\mathrm{Tr}_{\mathcal{A}_\mathcal{O}}\left[(\tau_s \otimes \mathbb{I})(\vec{m_1}.\vec{\Lambda})\right] \otimes \omega_t^T + \frac{(1-\nu)^2}{d^4}\mathrm{Tr}_{\mathcal{A}_\mathcal{O}}\left[(\tau_s \otimes \mathbb{I})\vec{m_1}.\vec{\Lambda}\right] \otimes \mathrm{Tr}_{\mathcal{B}_\mathcal{O}}\left[\vec{m_2}.\vec{\Lambda}(\mathbb{I} \otimes \omega_t)\right] \tag{37}$$

By knowing the character of the noise mixed with the measurement operator, the referee can change the $\beta_{s,t}$ values and in this way $I(\rho)$ remains proportional to $\mathrm{Tr}(W\rho)$. If he don't know that, then the error will be proportional to $\mathrm{Tr}[(W'' - W)\rho]$, where,

$$W'' - W = \sum_{s,t}\beta_{s,t}\left[\tau_s^{''T} \otimes \omega_t^{''T} - \tau_s^T \otimes \omega_t^T\right] \tag{38}$$

and, $\beta_{s,t}$ are calculated according to the equation [2].

With noisy input states and measurement operator

$$I(\rho) = I(\nu, \mu, \vec{m}_1, \vec{m}_2, \vec{n}_1, \vec{n}_2, \rho) = I(1, 1, \vec{0}, \vec{0}, \vec{0}, \vec{0}, \rho)$$

$$+\mathrm{Tr}\left[\rho\left(W'' - \sum_{s,t,a,b}\beta_{s,t}^{a,b}\tau_s^T \otimes \omega_t^T\right)\right] \tag{39}$$

So noise (both in preparation as well as measurement) can, in principle, degrade the quality of measurement device independent implementation of the entanglement witness operator.

B. Expression for $I_{\mathbf{mod}}(\rho_{\mathcal{AB}})$

Our original witnessing function was,

$$I(\rho_{\mathcal{AB}}) = \sum_{s,t} \beta_{s,t} \mathrm{Tr}\Big[\Big(|\Phi^+\rangle\langle\Phi^+|\otimes|\Phi^+\rangle\langle\Phi^+|\Big)(\tau_s\otimes\rho_{\mathcal{AB}}\otimes\omega_t)\Big] \tag{40}$$

and the modified form of that is,

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \sum_{s,t} \beta_{s,t}\ \xi\ \mathrm{Tr}\Big[(P_{\mathcal{A}_{\mathcal{O}}\mathcal{A}}\otimes P_{\mathcal{BB}_{\mathcal{O}}})(\tau_s\otimes\rho_{\mathcal{AB}}\otimes\omega_t)\Big], \tag{41}$$

where the modified measurement operators are given by,

$$\begin{aligned}
P_{\mathcal{A}_{\mathcal{O}}\mathcal{A}}\otimes P_{\mathcal{BB}_{\mathcal{O}}} &= \mu_1\mu_2\cos^2(\Delta_1)\cos^2(\Delta_2)|\Phi^+\rangle\langle\Phi^+|\otimes|\Phi^+\rangle\langle\Phi^+|\\
&+\mu_1\mu_2\cos^2(\Delta_1)\cos(\Delta_2)\sin(\Delta_2)|\Phi^+\rangle\langle\Phi^+|\otimes\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\\
&+\mu_1\mu_2\cos^2(\Delta_1)\sin^2(\Delta_2)|\Phi^+\rangle\langle\Phi^+|\otimes|\Psi^-\rangle\langle\Psi^-|\\
&+\frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1)|\Phi^+\rangle\langle\Phi^+|\otimes\mathbb{I}\\
&+\mu_1\mu_2\cos(\Delta_1)\sin(\Delta_1)\cos^2(\Delta_2)\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\otimes|\Phi^+\rangle\langle\Phi^+|\\
&+\mu_1\mu_2\cos(\Delta_1)\sin(\Delta_1)\cos(\Delta_2)\sin(\Delta_2)\\
&\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\otimes\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\\
&+\mu_1\mu_2\cos(\Delta_1)\sin(\Delta_1)\sin^2(\Delta_2)\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\otimes|\Psi^-\rangle\langle\Psi^-|\\
&+\frac{\mu_1(1-\mu_2)}{4}\cos(\Delta_1)\sin(\Delta_1)\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\otimes\mathbb{I}\\
&+\mu_1\mu_2\sin^2(\Delta_1)\cos^2(\Delta_2)|\Psi^-\rangle\langle\Psi^-|\otimes|\Phi^+\rangle\langle\Phi^+|\\
&+\mu_1\mu_2\sin^2(\Delta_1)\cos(\Delta_2)\sin(\Delta_2)|\Psi^-\rangle\langle\Psi^-|\otimes\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\\
&+\mu_1\mu_2\sin^2(\Delta_1)\sin^2(\Delta_2)|\Psi^-\rangle\langle\Psi^-|\otimes|\Psi^-\rangle\langle\Psi^-|\\
&+\frac{\mu_1(1-\mu_2)}{4}\sin^2(\Delta_1)|\Psi^-\rangle\langle\Psi^-|\otimes\mathbb{I}+\frac{(1-\mu_1)\mu_2}{4}\cos^2(\Delta_2)\mathbb{I}\otimes|\Phi^+\rangle\langle\Phi^+|\\
&+\frac{(1-\mu_1)\mu_2}{4}\cos(\Delta_2)\sin(\Delta_2)\mathbb{I}\otimes\Big(|\Psi^-\rangle\langle\Phi^+|+|\Phi^+\rangle\langle\Psi^-|\Big)\\
&+\frac{(1-\mu_1)\mu_2}{4}\sin^2(\Delta_2)\mathbb{I}\otimes|\Psi^-\rangle\langle\Psi^-|+\frac{(1-\mu_1)(1-\mu_2)}{16}\mathbb{I}\otimes\mathbb{I}
\end{aligned} \tag{42}$$

Therefore, from Equ. (40), (41) and (42) we have,

$$\begin{aligned}
I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \xi\Big[&\mu_1\mu_2\cos^2(\Delta_1)\cos^2(\Delta_2)+\frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1)\\
&+\frac{\mu_2(1-\mu_1)}{4}\cos^2(\Delta_2)+\frac{(1-\mu_1)(1-\mu_2)}{16}\Big]I(\rho_{\mathcal{AB}}) + \text{additional term}
\end{aligned} \tag{43}$$

Thus, both multiplicative and additive noises are present in the system.

Now, using Equ. (27) and (43), we have [for the choices $\mu_1 = \mu_2 = \mu$ and $\Delta_1 = \Delta_2 = \Delta$],

$$
\begin{aligned}
I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \ & \frac{\xi}{8} \sum_{s,t} \beta_{s,t} \Big[2a_3\mu \sin(2\Delta)x_t + 2a_1\mu \cos(2\Delta)x_t - 2a_2\mu y_t - 2a_1\mu \sin(2\Delta)z_t \\
& + 2a_3\mu \cos(2\Delta)z_t + 2b_1\mu(\cos(2\Delta)x_s + \sin(2\Delta)z_s) - 2b_3\mu(\sin(2\Delta)x_s - \cos(2\Delta)z_s) \\
& - 2b_2\mu y_s - 2c_{33}\mu^2 \sin^2(2\Delta)x_s x_t + c_{13}\mu^2 \sin(4\Delta)x_s x_t - c_{31}\mu^2 \sin(4\Delta)x_s x_t \\
& + 2c_{11}\mu^2 \cos^2(2\Delta)x_s x_t - 2c_{23}\mu^2 \sin(2\Delta)y_s x_t + 2c_{32}\mu^2 \sin(2\Delta)x_s y_t \\
& - 2c_{21}\mu^2 \cos(2\Delta)y_s x_t - 2c_{12}\mu^2 \cos(2\Delta)x_s y_t + 2c_{13}\mu^2 \sin^2(2\Delta)z_s x_t \\
& + 2c_{31}\mu^2 \sin^2(2\Delta)x_s z_t + c_{11}\mu^2 \sin(4\Delta)z_s x_t + c_{33}\mu^2 \sin(4\Delta)z_s x_t - c_{11}\mu^2 \sin(4\Delta)x_s z_t \\
& - c_{33}\mu^2 \sin(4\Delta)x_s z_t + 2c_{31}\mu^2 \cos^2(2\Delta)z_s x_t + 2c_{13}\mu^2 \cos^2(2\Delta)x_s z_t + 2c_{22}\mu^2 y_s y_t \\
& - 2c_{12}\mu^2 \sin(2\Delta)z_s y_t + 2c_{21}\mu^2 \sin(2\Delta)y_s z_t - 2c_{32}\mu^2 \cos(2\Delta)z_s y_t - 2c_{23}\mu^2 \cos(2\Delta)y_s z_t \\
& - 2c_{11}\mu^2 \sin^2(2\Delta)z_s z_t + c_{13}\mu^2 \sin(4\Delta)z_s z_t - c_{31}\mu^2 \sin(4\Delta)z_s z_t + 2c_{33}\mu^2 \cos^2(2\Delta)z_s z_t + 2 \Big]
\end{aligned}
\tag{44}
$$